Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: the "General Regulation"), and pursuant to the applicable legislation governing personal data protection, the Senate of the College of Management Bled, at its regular session 5/2023 held on 28 September 2023, adopted the following:

Personal Data Protection Regulations of the College of Management Bled

I. GENERAL PROVISIONS

Article 1

(1) These Regulations determine the organisational, technical and logical-technical procedures and measures for the protection of personal data within the organisation, with the purpose of preventing accidental or intentional unauthorised destruction, alteration or loss of data, as well as unauthorised access to, processing, use or disclosure of personal data.
(2) The responsible person of the organisation, management, employees, workers and all persons involved in the organisation's work process on the basis of an employment contract or any other contractual basis, who in the course of their work process and use personal and/or confidential data and/or become acquainted with the organisation's business secrets, shall comply with the provisions of the applicable legislation governing the field of personal data protection, the provisions of legislation governing their specific field of work, and the provisions of these Regulations.

Article 2

The terms used in these Regulations shall have the following meanings:

1. Identifiable natural person means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. Personal data filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
3. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
4. Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;
5. Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
6. Personal data means any information relating to an identified or identifiable natural person (hereinafter: "data subject");
7. Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status;

8. Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation;
9. Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
10. Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
11. Recipient means a natural or legal person, public authority, agency or another body to which personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union law or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
12. Controller means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union law or Member State law, the controller or the specific criteria for its designation may be provided for by Union law or Member State law.V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

II. PROCESSING OF PERSONAL DATA

Article 3

(1) Within the organisation, personal data may be processed on the basis of Article 6 of the General Regulation where at least one of the following conditions is fulfilled:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(2) Personal data may be processed only for specified and lawful purposes and may not be further processed in a manner incompatible with those purposes, unless otherwise provided by law.

(3) When processing special categories of personal data, employees shall exercise particular diligence and care. Special categories of personal data shall be protected in such a manner as to prevent unauthorised persons from gaining access to them.
(4) The data subject shall be informed of the processing of personal data in accordance with Articles 13 and 14 of the General Regulation, or shall be informed of his or her rights in accordance with Article 15 of the General Regulation.

Article 4

The data subject shall have the right to obtain from the organisation confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and the information referred to in Article 15(1) of the General Regulation. The organisation shall ensure the exercise of the following rights where the conditions laid down in the General Regulation are met:

- the right to rectification;
- the right to erasure ("right to be forgotten");
- the right to restriction of processing;
- the obligation of notification regarding rectification or erasure of personal data or restriction of processing;
- the right to data portability;
- the right to object and rights related to automated individual decision-making.

Article 5

(1) The responsible person of the organisation shall ensure that individuals are informed, in an appropriate manner and in accordance with the requirements of the General Regulation, of the rights referred to in the preceding Article of these Regulations. The responsible person shall also ensure a single contact point through which individuals may submit requests and communicate with the organisation regarding the exercise of their rights.
(2) As a rule, individuals shall have the following rights relating to the protection of their personal data:

- to request information as to whether the organisation holds personal data relating to them and, if so, which data, on what basis, and for what purpose;
- to request access to personal data, enabling them to receive a copy of the personal data held by the organisation and to verify whether the organisation processes such data lawfully;
- to request rectification of personal data, including the completion of incomplete or correction of inaccurate personal data;
- to request erasure of personal data where there is no longer any reason for further processing or where they exercise their right to object to further processing;
- to object to further processing of personal data where the processing is based on legitimate interests pursued by the organisation or a third party and grounds relating to their particular situation exist; irrespective of the foregoing, they shall have the right to object at any time where their personal data are processed for direct marketing purposes;
- to request restriction of the processing of personal data, meaning the suspension of processing, for example where they wish the organisation to verify the accuracy of the data or the grounds for further processing;
- to request the transfer of personal data in a structured electronic format to another controller, where possible and feasible;

- to withdraw consent previously given for the collection, processing and transfer of personal data for a specific purpose; upon receipt of notice of withdrawal, the organisation shall cease processing the personal data for the originally accepted purpose unless another lawful basis for processing exists.

(3) Where an individual wishes to exercise any of the above rights, he or she may submit a request to the Data Protection Officer by e-mail at dpo@datainfo.si or by post to DATAINFO.SI, d.o.o., Tržaška cesta 85, 2000 Maribor. Upon receipt of a request concerning the rights of an individual, information on the measures taken by the organisation shall be provided without undue delay and in any event within one month of receipt of the request. That period may be extended by a maximum of two additional months where necessary, taking into account the complexity and number of requests. The organisation shall inform the individual of any such extension within one month of receipt of the request together with the reasons for the delay.
(4) Access to personal data and the exercise of rights shall be provided free of charge. Where requests from an individual are manifestly unfounded or excessive, in particular because of their repetitive nature, the controller may charge a reasonable fee taking into account the administrative costs of providing the information, communication or action requested, or may refuse to act on the request.
(5) When exercising rights under this Chapter, the organisation may request certain information from the individual for the purpose of verifying his or her identity. This is a security measure intended to ensure that personal data are not disclosed to unauthorised persons.
(6) Where an individual considers that his or her rights have been infringed, he or she may seek protection or assistance from the supervisory authority, namely the Information Commissioner, at gp.ip@ip-rs.si, or obtain information on the website www.ip-rs.si.

Article 6

(1) Personal data shall be disclosed, at the request of a recipient, only to those recipients who demonstrate an appropriate legal basis or provide a written request or the consent of the data subject.
(2) Personal data shall be disclosed ex officio only to those recipients who have an appropriate legal basis.
(3) Disclosure of personal data under paragraph 1 of this Article may be requested by a recipient either in writing or orally. Where a written application is submitted, the recipient shall clearly specify the provision of law authorising the acquisition of the personal data or shall attach to the application a written request or the consent of the data subject. Where the recipient requests disclosure orally, the responsible person or authorised processor may, where there is doubt as to the existence of a written request or consent of the data subject, require the recipient to submit such written request or consent.
(4) Disclosure of special categories of personal data on the basis of paragraph 1 of this Article may be requested only in writing. The written application shall be identical in content to the written application referred to in the preceding paragraph.
(5) Personal data disclosed to a recipient in physical form shall be enclosed in a sealed envelope. The envelope shall ensure that it is not possible to open it and become acquainted with its contents without visible evidence that the envelope has been opened.
(6) Personal data may be transmitted by information, telecommunications and other means only where procedures and measures are implemented that prevent unauthorised appropriation or destruction of the data and unauthorised access to their contents.
(7) Special categories of personal data shall be sent in physical form to recipients in sealed envelopes against signature in the delivery register or by recorded delivery. Where special

categories of personal data are transmitted electronically, their unreadability during transmission shall be ensured by encryption and password protection.

Article 7

(1) The employee responsible for the receipt and registration of mail within the organisation shall deliver postal items containing personal data directly to the individual or department to whom the item is addressed. The same employee shall open and examine all postal items and consignments addressed to the organisation that arrive by other means (e.g. delivered by clients or couriers), except for the items referred to in paragraphs 2 and 3 of this Article.
(2) The employee responsible for the receipt and registration of mail shall not open items addressed to another authority or organisation that have been delivered in error, nor items marked as containing personal data or where the markings on the envelope indicate that they relate to a competition or a call for applications.
(3) The employee responsible for the receipt and registration of mail may open items addressed to both the organisation and an employee, except where it is evident from the envelope that the letter is to be served personally on the employee.

Article 8

(1) The organisation shall maintain a record of processing activities in accordance with the provisions of Article 30 of the General Regulation.
(2) Employees who process personal data shall be familiar with the record of processing activities. Access to the record of processing activities shall be granted to every employee upon request.
(3) The following shall be entered in the record of processing activities, where possible: the title of the personal data filing system, the purpose of processing, the legal basis, the categories of data subjects to whom the data relate, the types of personal data, the categories of recipients of personal data, transfers of personal data to a third country, the retention period, and a general description of the technical and organisational security measures.

Article 9

(1) Where it is possible that planned processing of personal data, in particular through the use of new technologies, taking into account the nature, scope, context and purposes of the processing of personal data, could result in a high risk to the rights and freedoms of individuals, the management of the organisation shall be alerted accordingly.
(2) In such a case, a data protection impact assessment shall be carried out, as provided for in Article 35 of the General Regulation.

Article 10

(1) For the purposes of documenting activities and informing the public about the work and events of the organisation, such as events, meetings, competitions, training sessions and similar activities, the organisation may audio-visually record or photograph such an event, either in whole or in part, and publish the resulting material on the organisation’s websites, in printed publications and on social media.
(2) Notice that an event will be recorded or photographed shall be included in the invitation or event notice. The purpose of the recording or photography shall also be stated. In this way, participants and visitors shall be deemed to have been informed that a public event will be recorded or photographed.
(3) Where this is more appropriate (for events with a smaller number of participants, events that are not open to the public, and where participants may reasonably expect a greater degree of

privacy), the recording or photography shall be announced orally and participants shall be given the opportunity to express their wishes regarding the capture of their image by camera.

Article 11

(1) The organisation shall regularly inform employees about the importance of and developments in the field of personal data protection and shall provide training in this field as well as in the field of information security.
(2) As a rule, once a year the organisation shall present the following to employees:

- the rights and obligations of employees regarding the protection of personal data;
- threats and the most common risks relating to the protection of personal data;
- possible consequences for the organisation and employees in the event of a personal data protection breach;
- password protection and password management;
- protection of equipment and premises;
- secure handling where data are taken outside the organisation's premises (e.g. on laptops, smartphones, USB flash drives and similar devices);
- the clean desk policy;
- other practices, policies and examples relating to personal data protection.

(3) The organisation shall regularly implement information security policies defined in internal acts and shall review them at least once a year.

III. DATA PROTECTION OFFICER

Article 12

(1) The responsible person of the organisation shall appoint a Data Protection Officer by decision or in another appropriate manner (e.g. by concluding a contract) and shall ensure that information concerning the Data Protection Officer is published on the organisation's website.
(2) The Data Protection Officer shall be appointed on the basis of professional qualities and, in particular, expert knowledge of personal data protection law and practice, and the ability to perform the tasks referred to in Article 39 of the General Regulation and the applicable legislation governing personal data protection.
(3) The organisation shall ensure that the Data Protection Officer is properly and promptly involved in all matters relating to the protection of personal data and that he or she is provided with the appropriate resources necessary for the proper performance of his or her tasks, as well as access to personal data and processing operations.
(4) The organisation shall ensure that the Data Protection Officer receives no instructions regarding the performance of his or her tasks.

Article 13

Data subjects may contact the Data Protection Officer regarding all matters relating to the processing of their personal data and the exercise of their rights under the General Regulation.

Article 14

In the performance of his or her duties, the Data Protection Officer shall be obliged to keep confidential all information acquired in the course of performing those duties, in accordance with the applicable national legislation.

Article 15

(1) The Data Protection Officer shall have at least the following tasks:

- informing the organisation, its processors and employees who carry out processing operations, and advising them of their obligations pursuant to the General Regulation and other legal provisions relating to the protection of personal data;
- monitoring compliance with the General Regulation and national legislation, including the assignment of responsibilities relating to personal data protection, awareness-raising and training of employees within the organisation who process personal data in the course of their work;
- providing advice, where requested, regarding the data protection impact assessment and monitoring its performance in accordance with Article 35 of the General Regulation;
- cooperating with the supervisory authority;
- acting as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the General Regulation and, where appropriate, consulting on any other matter.

(2) In the performance of his or her tasks, the Data Protection Officer shall have due regard to the risks associated with processing operations and shall take into account the nature, scope, context and purposes of the processing.

IV. CONTRACTUAL PROCESSING OF PERSONAL DATA

Article 16

(1) A written contract or other legal act under Union law or the law of a Member State shall be concluded with every external legal or natural person carrying out specific tasks relating to the processing of personal data on behalf of the organisation. Such contract or legal act shall define the processor's obligations towards the controller and shall specify the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and the obligations and rights of the controller. The content of such contract is further specified in Article 28 of the General Regulation.

(2) Processors shall also include external contractors who maintain hardware and software and who develop and install new hardware or software, where they have access to personal data in the course of their work.

(3) External legal or natural persons may carry out personal data processing services only within the scope of the organisation's authorisation and shall not process or otherwise use personal data for any other purpose.

(4) An authorised legal or natural person providing agreed services for the organisation outside the controller's premises shall ensure a level of personal data security at least as stringent as that prescribed by these Regulations.

V. ERASURE OF DATA

Article 17

(1) Personal data may be processed only for as long as the retention period is prescribed or for as long as a legal basis under Article 6 of the General Regulation exists. Upon expiry of the retention period, personal data shall be erased, destroyed, blocked or anonymised, unless otherwise provided by law or another act.

(2) Personal data processed by the organisation on the basis of a contractual relationship with a data subject shall be retained for the period necessary for the performance of the contract and for a further six years following its termination, except where a dispute relating to the contract arises between the data subject and the organisation. In such a case, the organisation shall retain the data for a further six years following the final court judgment, arbitration award

or settlement, or, where no judicial proceedings have taken place, for six years from the date of the amicable settlement of the dispute.
(3) Personal data processed by the organisation on the basis of the data subject's consent or legitimate interest shall be retained until such consent is withdrawn or until a request for erasure is submitted. Upon receipt of the withdrawal or request for erasure, the data shall be erased without undue delay and, in any event, within one month of receipt of the request. That period may, where necessary, be extended by a maximum of two additional months, taking into account the complexity and number of requests, of which the data subject shall be informed. The organisation may also erase such data prior to withdrawal where the purpose of the processing of personal data has been achieved or where so required by law.
(4) Exceptionally, the organisation may refuse a request for erasure on the grounds set out in the General Regulation, namely:

- the exercise of the right to freedom of expression and information;
- compliance with a legal obligation requiring processing;
- reasons of public interest in the area of public health;
- archiving purposes in the public interest;
- scientific or historical research purposes or statistical purposes;
- the establishment, exercise or defence of legal claims.

Article 18

(1) For the erasure of data from data storage media, a method of erasure shall be used that makes the recovery of all or part of the erased data impossible.
(2) Data stored on conventional media (documents, card indexes, registers, lists, etc.) shall be destroyed in a manner that makes it impossible to read all or part of the destroyed data. Supporting materials (e.g. matrices, calculations and charts, sketches, draft or unsuccessful printouts, etc.) shall be destroyed in the same manner.
(3) It shall be prohibited to dispose of waste data storage media containing personal data in waste bins. During the transfer of media containing personal data to the place of destruction, appropriate security measures shall also be ensured throughout the transfer process. The transfer of data storage media to the place of destruction and the destruction of media containing personal data shall be supervised by a special committee, which shall draw up an appropriate record of destruction, or the destruction shall be entrusted to an appropriate external service provider on the basis of a concluded contract. (1) Za brisanje podatkov iz nosilcev podatkov se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

VI. INFORMATION SECURITY POLICY

Article 19

(1) Employees shall use various information technology devices (computer, telephone, tablet and other electronic devices) and various electronic services (Internet access, electronic mail, cloud access, shared directories and folders, and other software or services) assigned to them by the employer exclusively for business purposes.
(2) Information technology and electronic services assigned by the organisation may also be used for private purposes to a limited extent and within reasonable limits. In doing so, employees shall protect the reputation of the organisation, and the technologies and services shall not be used for inappropriate or offensive purposes. The management may, at its sole discretion, prohibit an employee from using them for private purposes at any time.

Article 20

(1) Access to the World Wide Web shall be provided to employees for the purposes of their work, education and information.

(2) Employees of the organisation shall use the World Wide Web in accordance with ethical and moral standards. All users of information systems shall be aware that, when using the Internet, they identify themselves through the network address of the public institution (IP address).

(3) The forwarding of official e-mail addresses to external web servers for the purpose of registering for a specific service (e.g. e-mail services, registration for training courses, etc.) shall not be permitted unless it is connected with the organisation's business process.

(4) Within the organisation's network, statistics on visited websites may be generated at the request of the responsible person. Such statistics shall be anonymised and shall not be intended for public disclosure. The statistics may be used exclusively for the planning and protection of the information system.

(5) For the purpose of ensuring information security and the availability of information resources, and for the prevention of violations, the management of the organisation may, by means of a special order, direct that access to specific websites be blocked. The blocking of access to specific websites shall be carried out by the person responsible for the operation of the computer information system on the basis of a written order issued by the responsible person. All employees shall be informed of such blocking by electronic mail.

Article 21

(1) Official electronic mail within the organisation may be used as a communication tool with parents, pupils/students, clients, employees and external contractors. In doing so, employees shall comply not only with ethical and moral standards but also with the rules of business etiquette. The sender shall be aware that any message sent from an official e-mail address may be regarded by the recipient as the opinion of the organisation in which the sender is employed.

(2) Employees shall not send chain letters or large files (music, films, performances, executable files, scripts, etc.) by electronic mail unless such files are required for work purposes.

(3) Employees shall not use their official e-mail address for marketing purposes and shall not send advertising messages from that address to known and/or unknown recipients. Employees shall likewise not subscribe to advertising mail or newsletters using the organisation's e-mail addresses unless such subscription is connected with the requirements of their position.

(4) Employees shall exercise caution when opening electronic mail containing attachments from unknown senders. Where there is a suspicion that a message constitutes unsolicited mail that may be harmful, it shall not be opened; instead, the competent person responsible for the operation of the computer information system shall be informed.

(5) Employees shall under no circumstances send special categories of personal data or passwords by electronic mail, except through appropriately accredited systems. Alternatively, the unreadability of the data during transmission shall be ensured by encryption and password protection. (1) Zaposleni uporabljajo različno informacijsko tehnologijo (računalnik, telefon, tablica in druge elektronske naprave) ter različne elektronske storitve (dostop do interneta, elektronska pošta, dostop do oblaka, skupni imeniki in mape ter drugo programsko opremo oziroma storitve), ki jim jo dodeli delodajalec, izključno za službene namene.

Article 22

(1) Remote access to the organisation's information system shall be permitted only on the basis of an approved method providing an appropriate level of security, and only for those

employees who require such access for the performance of their work duties, and only to a limited extent. The clean screen policy shall also be observed. Upon completion of work, the user shall log out of the system and ensure that no data or traces remain at the workstation.
(2) For the implementation of secure remote access, hardware shall be equipped with appropriate software recognition mechanisms enabling protection of the endpoint against internet threats. In order to ensure confidentiality, all traffic from the remote network endpoint to the organisation's network shall be encrypted.

Article 23

(1) The person responsible for the operation of the information system within the organisation may, upon a specifically justified written request by the authorised person and in the presence of a three-member committee, in exceptional circumstances (sudden resignation of an employee, death of an employee, unexpected, sudden and prolonged or permanent absence of an employee, termination of employment by the employee without notice, termination of employment for reasons attributable to the employee due to unjustified absence, and in similar exceptional cases), inspect an employee's information technology (e.g. a computer) or other electronic services (e.g. electronic mail), but only where this is strictly necessary for the fulfilment of the organisation's legal obligations or for the management of the work process.
(2) The inspection shall be carried out by a three-member committee appointed on each occasion by the organisation's authorised person. At least one member of the committee shall be a representative of the employees who is not a managerial employee. The committee shall prepare a record of the inspection containing:

- an explanation of the reasons for the inspection;
- a record of entry, including any comments made by the employee, where present;
- details of the persons present;
- a list or printout of the data obtained.

(3) Where there are reasonable grounds for suspecting that employees are not complying with the information security policy laid down in these Regulations, the person responsible for the operation of the computer information system may, upon a specifically justified written request by the responsible person, carry out monitoring of the use of electronic services, solely by reviewing log records relating to the volume of traffic and stored data placing a load on the server. The content itself shall not be examined.
(4) The organisation may request access to the telephone traffic data of connections owned by the organisation from telecommunications service providers or the maintainer of the internal telephone exchange only where a dispute arises between the organisation and an employee regarding the amount of costs incurred through the use of a specific telephone connection.
(5) Employees shall be informed in writing of the purpose of the use of information technology and electronic services under this Article and of the possibility of inspection. Notification sent to all employees by electronic mail together with these Regulations shall be deemed sufficient notification.

Article 24

Upon termination of employment or upon exhaustion of the basis for the performance of work, an employee of the organisation shall return the information technology equipment provided for official purposes that he or she has used for work purposes. Prior to returning such equipment, the employee shall ensure that all private content has been removed or deleted from the information and electronic services used, while all official content shall be retained in its entirety.

Article 25

(1) For the purposes of performing work, an employee may, in addition to official equipment, use his or her own private equipment and other technical devices (in particular a mobile telephone), provided that such use is approved by the responsible person and the employee gives voluntary written consent allowing the employer, for the purposes of carrying out the work process, to process his or her private telephone number or private e-mail address.

(2) In the event of termination of employment, the employee shall delete from private equipment or other devices and their data storage media, which were used for official purposes with the employer's consent, all personal data transferred in the course of the work process and all files used by the employee for official purposes, irrespective of whether such files contain personal data.

VII. PROTECTION OF PREMISES AND COMPUTER EQUIPMENT

Article 26

(1) Premises in which personal data storage media, hardware and software are located (secured premises) shall be protected by organisational, physical and/or technical measures preventing unauthorised persons from accessing the data.

(2) Secured premises shall include management or administration offices, the secretariat, server rooms, programming and maintenance service rooms, offices, consulting rooms and other premises to which unauthorised persons are not permitted access.

(3) Access to secured premises shall be permitted only during normal working hours and outside those hours only on the basis of authorisation granted by the responsible person of the organisation.

Article 27

In premises intended for conducting business with clients or which do not have the status of secured premises and to which access by non-employees is permitted (e.g. the reception office, secretariat), data storage media and computer screens shall be positioned in such a way that clients do not have direct access to their contents. In such premises, notice boards or any other means of display shall not contain data on the basis of which unauthorised persons could become acquainted with the personal data of an individual where the organisation has no legal basis for their publication.

Article 28

Maintenance and repair of information technology, electronic services and other equipment shall be permitted only with the knowledge of the responsible person, and may be carried out only by authorised service providers or maintenance personnel who have concluded an appropriate contract with the organisation.

Article 29

Maintenance personnel for premises, information technology, hardware and software, visitors and business partners may enter and move within secured premises only with the knowledge of the responsible person. Employees such as cleaners, security guards and others may, outside working hours, enter and move only within those secured premises where access to personal data is prevented (data storage media are stored in locked cabinets and desks, computers and other hardware are switched off or otherwise physically or software locked).

VIII. PROTECTION OF SYSTEM SOFTWARE AND APPLICATION SOFTWARE

Article 30

Access to electronic services and software shall be protected in such a manner that access is permitted only to employees of the organisation designated in advance for that purpose or to external associates – natural or legal persons who provide agreed services in accordance with a contract.

Article 31

Amendments, modifications and upgrades to system software and application software shall be permitted only on the basis of approval granted by the responsible person or a person authorised by him or her. Such activities may be carried out only by an authorised service provider or maintenance provider who has concluded an appropriate contract with the organisation.

Providers shall appropriately document all amendments, modifications and upgrades made to system software and application software. Where copies must be made for the purpose of carrying out the work, such copies shall be appropriately destroyed once the purpose for which they were made has ceased to exist. The same shall apply to all other printouts, data exports or other tools used for the provision of maintenance services.

Article 32

(1) The contents of data storage media located on network servers and local workstations containing personal data shall be regularly checked for the potential presence of computer viruses and other forms of malicious code. Where a virus is detected, it shall be removed by the appropriate specialist service or the competent person responsible for the operation of the computer information system, and efforts shall simultaneously be made to determine the cause of the virus occurrence.

(2) All personal data and software intended for use within the computer information system and received by the organisation on computer data transfer media or through telecommunications channels shall, prior to use, be checked for the presence of computer viruses.

Article 33

Employees shall not install software without the approval of the person responsible for the operation of the computer information system. They shall likewise not remove software from the organisation without the approval of the responsible person of the organisation or the head of the organisational unit and without the knowledge of the person responsible for the operation of the computer information system.

Article 34

(1) Access to data and the use of system and application software shall be protected by a password system for the authorisation and identification of users of software and data. Each user shall have his or her own password for access to individual electronic services. Lending passwords and the use of shared passwords shall be prohibited.

(2) When generating or determining passwords, the following rules shall be observed:

- passwords shall consist of a minimum of 8 characters or be correspondingly longer where this is specified for a particular user solution;
- passwords shall not contain meaningful alphanumeric character sequences (e.g. 123456, abcdefg...);
- passwords shall be of adequate quality (appropriate length, upper-case and lower-case letters, numbers and, where applicable, special characters);
- passwords should not be cyclical and should not be repeated from previous periods;

- mandatory regular password changes shall be implemented (at least every 6 months);
- initial passwords shall be changed upon first log-in;
- passwords generated by an external supplier shall be changed immediately upon first use in the production environment;
- the user name shall not indicate the user's special authorisations.

(3) The following instructions shall be observed when handling passwords:

- the authorised person assigning passwords shall treat them as confidential, prevent the possibility of unauthorised access to them and communicate them in a secure manner;
- users shall be enabled to change their user password at any time;
- a password shall never be displayed on the screen;
- passwords shall be stored in encrypted form;
- passwords shall not be attached to a monitor or stored under a keyboard;
- each user shall have his or her own user name and password exclusively for personal use;
- a password shall be stored in a manner that completely prevents any other person from viewing it;
- each user shall be responsible for maintaining the confidentiality of the password and shall not disclose it to any other person under any circumstances;
- under no circumstances shall a user disclose a password to a superior, subordinate, substitute person or IT personnel;
- in the event of disclosure of a password, or suspicion of such disclosure, the user shall immediately notify the authorised person responsible for assigning passwords.

(4) All passwords and procedures used for access to and administration of the personal computer network (supervisory or control passwords), administration of electronic mail and administration of application software shall be stored in a safe in a sealed envelope or in another appropriate manner so that access by unauthorised persons is prevented. They shall be used only in exceptional circumstances or emergency situations. Any use of such passwords may be authorised only by the responsible person of the organisation. Following each such use, new passwords shall be established.

Article 35

(1) For the purposes of restoring the computer system in the event of failures and other exceptional situations, backup copies of data shall be created regularly.

(2) Backup copies of data shall be stored in locked fire-resistant cabinets and protected against flooding and electromagnetic interference.

IX. ACTIONS IN THE EVENT OF SUSPECTED UNAUTHORISED ACCESS

Article 36

(1) Employees are obliged to immediately inform the authorised person of activities related to the detection of, unauthorised access to or destruction of data, malicious or unauthorised use, appropriation, alteration or damage, and shall themselves attempt to prevent such activity.

(2) A personal data protection breach means a security breach resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A breach may be committed unintentionally (e.g. through negligence) or intentionally. In general, such a breach constitutes a security incident that compromises the confidentiality, integrity and availability of personal data.

(3) Employees are obliged, in the course of their work, to monitor and be attentive to potential security incidents and to act accordingly in accordance with this Policy.

Article 37

(1) As soon as employees become aware that a security incident has occurred within the organisation, they must immediately notify their superior or the management of the organisation.
(2) The management must first determine what has occurred, assess what the potential adverse consequences are for the rights and freedoms of individuals, and take appropriate measures to remedy the consequences or at least reduce risks. It is recommended that the management consult the Data Protection Officer when preparing an assessment of the likelihood and severity of consequences for the rights and freedoms of individuals.
(3) In the event that the management of the organisation assesses that the incident is likely to result in a risk to the rights and freedoms of individuals, it must notify the Information Commissioner without undue delay, and at the latest within 72 hours of becoming aware of the breach. In the event that the incident concerns data for which the organisation acts as a processor, it must notify the controller as soon as possible after becoming aware of the breach.
(4) The notification shall be made using the form recommended by the Information Commissioner, which forms part of the organisation's documentation. Upon notification, the Information Commissioner must obtain at least the following information, as required by the General Regulation:

- a description of the nature of the breach, the categories and approximate number of individuals concerned, and the types and approximate number of personal data records;
- contact details of the Data Protection Officer;
- a description of the likely consequences of the personal data protection breach;
- a description of measures taken or proposed measures by the controller to mitigate risks arising from the breach.

Article 38

(1) The responsible person of the organisation is responsible for notifying the Information Commissioner of personal data protection breaches pursuant to Article 33 of the General Regulation.
(2) Detailed measures in the event of suspected unauthorised access to personal data are regulated in the document: Instructions for handling and responding to personal data protection breaches.

X. RESPONSIBILITY FOR IMPLEMENTING SECURITY MEASURES AND PROCEDURES

Article 39

(1) All employees of the organisation, as well as external contractors who have signed a cooperation agreement with the company, are responsible for implementing procedures and measures for the protection of personal data.
(2) Supervision over the implementation of procedures and measures determined by this Policy shall be carried out by the responsible person of the organisation, or a person authorised by them.

Article 40

Every employee who processes personal data is obliged to implement prescribed procedures and measures for data protection and to safeguard data of which they have become aware or with which they have been familiarised in the course of their work. The obligation to protect data does not cease upon termination of the employment or other contractual relationship.

Article 41

(1) In the event of a breach of the provisions of this Policy, the employee shall be liable in damages to the organisation for any harm caused to the organisation or to natural or legal persons with whom the organisation cooperates.
(2) A breach of the provisions of this Policy constitutes a serious breach of employment obligations under the employment contract or a substantial breach of another contract, on the basis of which the organisation may terminate the employment contract or other contract forming the basis for work performed for or within the organisation.
(3) A breach of the provisions of this Policy may result in criminal, minor offence and/or damages liability of the employee or person breaching this Policy.

XI. FINAL PROVISIONS

Article 42

(1) Employees of the organisation are informed of this Policy by publication on the notice board and/or intranet of the organisation and by sending it to all employees via electronic mail. Employees of the organisation may familiarise themselves with the content of the Policy at any time upon request submitted to the responsible person of the organisation.
(2) On the date of adoption of this Policy, the existing Personal Data Protection Policy shall cease to apply.

This Policy shall enter into force on the day following its adoption by the Senate of the Bled School of Management and shall be published on the website of the Bled School of Management.

Reference number: VM-P-016/2023
Date: 28 September 2023

Chair of the Senate of VM Bled
mag. Tadeja Krašna